Tip Sheet

Securing your home or office Wi-Fi

Wi-Fi is a cheap and easy way to connect your devices to each other and to the internet without running cables throughout your home or office. However, because Wi-Fi is sent through the air, it's important to take steps to secure your network and devices.

About your Wi-Fi network
A basic Wi-Fi network involves two key pieces of equipment, in addition to the computers and mobile devices you connect to the network:

- A **wireless access point** connects various devices on your wireless network; for example if you stream music wirelessly from a computer to a set of speakers, this happens over the access point.
- A **router** connects devices on your wireless network to an outside network, such as the internet. When you send an email, the data goes over your wireless network, through the access point, and then through the router.

The **wireless access point** and **router** are often combined into one unit called a **wireless router**, sometimes called a *wireless modem/router* or a *gateway.*

Choose a new router password
As a first step you should change the router's login password. To change the configuration of your wireless router, you need to log onto the *Admin* page for the router with a username and password using a web browser. Instructions on how to do this will be in your router's manual.

Wireless routers are sold with default passwords set up. Leaving the default password in place is a security risk as devices sold by some manufacturers will have the same password, making it easy for someone to find out the default password and use it to log on to your router and gain control of your network.

Use wireless security
Wireless routers can encrypt wireless network traffic so that only authorised devices can read the data. You should use *WPA* or *WPA2* security (WEP is no longer secure). For simple networks, the usual way to run WPA is in *WPA pre-shared key* (*WPA-PSK*) mode.

When you activate one of these protocols, you will have to choose a **passkey** for the network. This should *not* be the same as the login password to your wireless router as anyone with the passkey can then access your wireless router and take control of your network. The first time someone connects to your network, they will need the **passkey** to gain access.

WPA and WPA2 encyption makes network traffic unreadable to people who don't have the passkey.

Australian Communications Consumer Action Network (ACCAN)
Australia's peak body representing communications consumers

Suite 4.02, 55 Mountain St, Ultimo NSW 2007
Tel: (02) 9288 4000 | TTY: (02) 9281 5322 | Fax: (02) 9288 4019
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

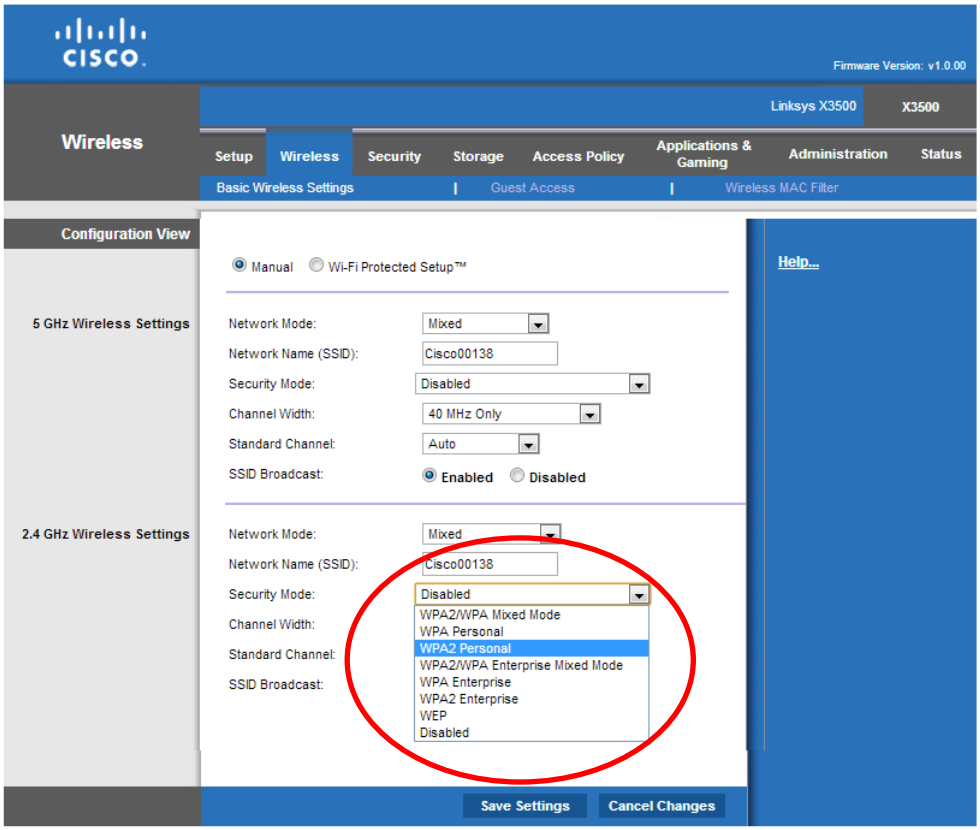

Figure 1: Sample wireless network configuration screen with wireless security option highlighted ('security mode')

Set up a firewall

Most routers have inbuilt firewalls that can be used to restrict unsolicited incoming internet traffic, while letting through web pages, email, or other information requested by your computer(s) or mobile devices. Unless you have a specific reason to change the settings of your router's firewall, it's usually best to leave it on with the default settings.

Turn off unnecessary functions

Some wireless routers will have a range of services available that allow you to remotely configure your router, computers, or remotely access your files. Unless you have a reason to run these services, you can minimise security risks by disabling them.

Restrict devices by hardware address

All devices with networking capabilities (like a computer or mobile phone) have a *hardware address* (sometimes called a 'MAC' address). A hardware address is made up of six pairs of letters and numbers, for example. '01:22:A5:CC:40:9F'. These addresses are difficult to change, and so they can be used to identify authorised devices.

Most wireless routers can limit access to devices with particular MAC addresses. This is a very secure way to stop unathourised devices connecting to your network, but it is only useful if you know all the devices that will regularly use your wireless network. If you often want to share your network with unknown devices, this type of access control is difficult to manage.

Authenticate your users

If you run a small business, you might want additional security. One way to get this is to use *WPA-Enterprise* mode. This requires a RADIUS server that assigns each user their own network encryption key. It offers more security than WPA-PSK, but it is also more complex and, depending on your needs, may be unnecessary.